

REMARKS/ARGUMENTS

Claims 1-4, 6-10, 12-15, 17-36, 38-59, and 61-64 remain in the patent application and claims 65-68 are added by this response. Claim 5 was previously cancelled and claims 11, 16, 37, and 60 are canceled by this amendment.

Claims 1, 34, and 55 are amended to distinctly describe the subject matter of the invention and to incorporate limitations originally appearing in claims 11, 16, 37 and 60. The additional limitations brought into the independent claims place the claims in better condition for consideration on appeal and because they appear in dependent claims as filed these amendment do not raise any new issues that would require further research by the examiner. Accordingly, the amendments should be entered under 37 C.F.R. 1.116.

A. Premature Final Rejection

The final office action states a rejection of claim 37 for the first time based upon the Russell-Falla et al ("Russell-Falla") reference. This rejection was not stated anywhere in the prior office action mailed June 17, 2004. Applicant has not, until now, had an opportunity to address the limitations of claim 37 and so have been denied a full and fair hearing required by MPEP 706.07. It is respectfully requested that finality of the office action be reconsidered and withdrawn.

B. Oath/Declaration

A substitute oath will be provided upon indication of allowable subject matter.

C. Rejections under 35 U.S.C 112

The objection characterizes the term "TCP/IP" in a manner that may be construed as technically inaccurate. TCP/IP as used in the claims refers to the transmission control protocol, which is a transport layer protocol, in combination with Internet Protocol which is a network layer protocol. The amendment to claim 1 is believed to overcome the rejection stated in the Office action. It is respectfully

requested that the rejections be withdrawn.

The Office action states in paragraph 18 at the bottom of page 5 that "half-sessions" are inherent in any network. On the other hand, the Office Action states in paragraph 15 that claims 1 and 34 are indefinite because they use the term "half-sessions". How can the use of a term that is admittedly inherent in the subject matter being claims be indefinite? It is respectfully requested that the rejection under 35 U.S.C. 112 be withdrawn.

With respect to the term "half-session", the term is not used in the specification to refer to the proprietary IBM SNA protocol. Further, the interpretation suggested in the Office action (i.e., "part of network communications that are incoming communications") is misleading. The term "half-session" is used in the specification and claims in a manner that is consistent with its ordinary meaning to refer to the set of messages sent from a first user of a pair to the second user of the pair. The attached article, entitled "TCP Protocol Overview" states that "TCP data is organized as a stream of bytes...." The article describes full-duplex operation of TCP as well noting that it is "sometimes useful to think of a TCP session as two independent byte streams, traveling in opposite directions." The term "half-session" appearing in the claims refers to one of these two independent byte streams.

It should be noted that at a given machine, the transport-layer protocol components see both half-sessions that make up a particular session. In other words, the TCP layer sees both an incoming half-session and an outgoing half-session. As noted in the Office action, the existence of half-sessions is inherent at a protocol layer that is session-aware. What is not inherent is the decision to store and use half sessions in the manner called for in claims 1 and 34. A TCP half session is not simply an arbitrary collection of packets. A TCP half-session is a coherent assembly of a set of packets (which are referred to as "segments" in the IETF TCP protocol specification RFC793) in which the various packets are have a sequence with respect to each

other.. This coherent assembly is a meaningful form of the data that the inventors have discovered allows for analysis to be more accurate.

By way of a specific example, consider an instance in which a sensitive document containing vital company secrets might be transmitted over a TCP connection. The TCP connection might be transporting email, instant messaging, FTP traffic, or other protocol, any of which might be used to transport the document. The document contains text information such as "company confidential" and "proprietary do not distribute" occurring on each page. Hence, the document has multiple clues sprinkled throughout that could be used to detect a breach of company policy.

However, because the keywords are sprinkled throughout the documents, any particular TCP packet is unlikely to contain the keywords. Occasionally a packet might be found to contain one of the keywords, however, raising an alarm each and every time the word "proprietary" occurs in a TCP packet would lead to many false positives. It is not the single occurrence of "proprietary confidential" in any given packet that indicates a breach. The inventor has recognized that it is the multiple occurrences of a given criteria in a single document that is a better indicator of a breach. Since a TCP half-session will contain large portions of the document, if not the entire document, storing the half session has been found to provide a distinct advantage in reducing false positives when subsequently testing the stored communication. At the same time, the stored half-session allows the subsequent analysis to be refined because the data being transmitted can be tested in a much larger context.

The Office action states in paragraph 18 at the bottom of page 5 that "half-sessions" are inherent in any network. On the other hand, the Office Action states in paragraph 15 that claims 1 and 34 are indefinite because they use the term "half-sessions". How can the use of a term that is admittedly inherent in the subject matter being claimed be indefinite? It is respectfully requested that the rejection under 35 U.S.C. 112 be withdrawn.

D. Rejections under 35 U.S.C 102

Claims 34-35, 37-39, 44, 47-50, 52-55, 57, 58, and 60-64 were rejected under 35 U.S.C. 102 based upon the Russell-Falla. This rejection is respectfully traversed.

Claim 34, as amended, clarifies that the predetermined expressions are defined by a user (e.g., an network administrator, IT specialist, and the like) At least this feature of claim 34 is not shown or suggested in the relied on reference. Russell-Falla does not suggest any means by which the user can define expressions for use in testing as called for in original claim 16 and now in claim 34. Instead, Russell-Falla determines the contents of database 30 by a neural network or other automated analysis of large numbers of content examples. Applicants have found that the complexity of this analysis can be avoided by allowing a user to define predetermined expressions, as called for in claim 34. Moreover, user-defined criteria enable the user to express control and purpose in the defined criteria and so enable improved performance.

Claim 34 calls for, among other things, removing data content that does not contain language elements. The Office action cites a portion of Russell-Falla that relates to scanning an HTML page for regular expressions. It appears that the entire HTML page is used as input for analysis, including non-language elements. Russell-Falla does not show or suggest any activity of removing data content that does not contain language elements.

Further, the Russell-Falla reference does not show or fairly suggest capturing data on a network comprising multiple half sessions of TCP/IP network communications. An HTML page comprises text data extracted from one or more TCP packets that are assembled at the browser according to the HTML rules. HTML is a markup language, not a protocol. Accordingly, an HTML page does not, by itself, define a "session" or "half session". An HTML page, like any computer file, may be delivered over a network communication protocol, however, the HTML page is itself entirely independent of any particular network communication protocol. Hence, an

HTML page is by and intent design entirely unaware of any concept of "session" that exists on the network itself and so cannot satisfy the claim limitation "wherein the data comprises multiple half sessions..." appearing in claim 34.

The HTML page is distinct from a TCP/IP half session. Significantly, the a TCP/IP (or other network level) communication typically includes a wide variety of non-HTML information. This data may include header information, cookies, parameter information, and the like. In some cases the network communication may include malicious (or benevolent) code or hidden data that "piggy backs" on the network communication packets used to deliver an HTML page. This is equally true of other applications such as email, instant messaging, and the like. This piggy backed data is not a part of the HTML page in Russell-Falla, but it is a part of the captured half session in claim 34. Hence, this data will escape analysis in Russell-Falla, but will be subject to monitoring by the invention of claim 34.

Further, claim 34 calls for maintaining a sum of values associated with said predetermined expressions found within at least one category. Russell-Falla does not show or suggest the use of categories nor maintaining a sum of values on a category basis as called for in claim 34. The amendments to claim 34 are believed to clarify the use of multiple categories in claim 34. The Office action asserts that Russell-Falla does not prohibit multiple categories. However, this is far different from actually teaching multiple categories and the particular act of maintaining a sum of values on a category basis called for in claim 34. Russell-Falla must positively teach, not just fail to prohibit, this feature of claim 34 to form a rejection under 35 U.S.C. 102. For at least these reasons claim 34 is allowable over Russell Falla.

Claims 35, 37-39, 44, 47-50, 52-54 are allowable for at least the same reasons as claim 34 set out above.

Claim 55 calls for, among other things, "defining categoriess with weighted predetermined expressions" (emphasis added) and "maintaining a sum of values

associated with said predetermined expressions found within each category.” These features of claim 55 are not shown or suggested in the relied on reference. As noted hereinbefore and admitted in the Office action, Russell-Falla does not teach plural categories. Applicant maintains the position that Russell-Falla teaches away from using multiple categories. Moreover, if one were to modify Russell-Falla as suggested in the Office action, one might, by happenstance or invention, come up with the solution called for in claim 55. However, that solution is not taught or suggested by the reference itself. Further, claim 55 calls for storing the remaining data if the sum of values associated with said predetermined expressions present within a category exceeds a threshold value. For at least these reasons claim 55, and claims 57, 58, and 60-64 are allowable over Russell-Falla.

E. Rejections under 35 U.S.C 103

Claims 1-4, 6, 7, 11-13, 15-21, 23, 27-29, 32 and 33 were rejected under 35 U.S.C. 103 based upon Russell-Falla. in view of Trcka. This rejection is respectfully traversed. Claims 1-4, 6, 7, 11-13, 15-21, 23, 27-29, 32 and 33 are distinct from Russell-Falla for at least the same reasons stated above.

Claim 1 calls for monitoring network communications wherein each network communication comprises multiple half sessions, then storing at least some of the half sessions on disk. An HTML page in Russell-Falla is by design distinct and independent of a session at the network communication level. Analyzing an HTML page is not fairly construed as monitoring TCP/IP network communications. Trcka does not supply this deficiency. Trcka stores raw data packets at a network communication at a data link or lower level (e.g., Ethernet packets or lower). This is data below the transport level, and below the TCP/IP level called for in claim 1.

Trcka does not teach any specific type of analysis that would be performed on the raw data packets. Hence, Trcka does not teach the step of testing the stored communication for the presence of at least one user-defined criterion.

Further, claim 1 calls for storing the communication in a conditional manner, "if the presence of at least one preselected criterion is determined." Trcka teaches that all raw data packets are stored, not a process of storing some and deleting some as called for in claim 1. Russell-Falla does not explicitly teach storing any of the communication. Accordingly, the combination of Russell-Falla and Trcka does not suggest the invention of claim 1.

Moreover, there is no teaching in the references as to how such a combination would be achieved. The references appear to teach against the combination suggested in the office action. Russell-Falla deals with analyzing a web page before it is displayed whereas Trcka specifically captures data passively without interrupting delivery. Russell-Falla must analyze HTML pages, not network packets, whereas Trcka must capture network packets at a very low level. The two references, as taught in the references themselves, describe incompatible systems. Only applicants have recognized and invented a way for performing text analysis akin to what Russell-Falla is doing on HTML pages in an offline manner within a network connection, akin to what Trcka is doing at a data link layer.

Claims 6, 7, 11-13, 15-21, 23, 27-29, 32 and 33 are allowable for at least the same reasons as claim 1 from which they depend as well as the individual limitations appearing in those claims.

Claims 30 and 31, which depend from claim 1, are allowable over the combination of Russell-Falla and Trcka for at least the same reasons stated above.

Claims 36, 51 and 59 were rejected under 35 U.S.C. 103 based upon Russell-Falla. This rejection is respectfully traversed. Claims 36, 51 and 59 are allowable over Russell-Falla for at least the reasons stated above with respect to claims 34 and 55.

Claims 8-10, 14, 22 and 24-26 were rejected under 35 U.S.C. 103 based upon Russell-Falla. in view of Rajaraman et al ("Rajaraman"). This rejection is respectfully

traversed.

Rajaraman do not supply the deficiencies of Russell-Falla noted above. With respect to claim 1 specifically, the Rajaraman reference does not show or suggest monitoring TCP/IP layer communications, storing half sessions to disk or the use of plural categories as noted above. Rajaraman involves searching hierarchical data that has already been categorized. Claims 8-10, 14, 22 and 24-26, on the other hand, involve hierarchical weighted scoring of data for the purpose of subsequent categorizing. For at least these reasons it is respectfully requested that the rejection of claims 8-10, 14, 22 and 24-26 be withdrawn.

Claims 40-43, 45, 46 and 56 were also rejected under 35 U.S.C. 103 based upon the Russell-Falla in view of Rajaraman. This rejection is respectfully traversed. Rajaraman does not supply the deficiencies of Russell-Falla noted above with respect to claim 34 and claim 55 from which these claims depend. It is respectfully requested that the rejection be withdrawn.

F. New claims 65-68

New claims 65-68 are added by this amendment. Support for claims 65-67 appears at page 5, lines 10-16 and for claim 68 in the text bridging pages 4 and 5. These claims are believed to be allowable for at least the same reasons as claim 1 from which they depend. Moreover, the combined references do not show or suggest handling multiple independent data streams within a TCP/IP session in the manner called for in claims 65-67. Nor do the references show or suggest protocol identification. Russell-Falla do not involve protocol-based analysis at all, and Trcka dos not distinguish between protocols in any analysis. For these reasons claims 65-68 are allowable.

G. Conclusion

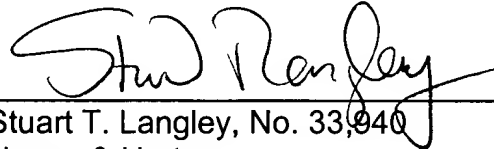
In view of all of the above, the claims are now believed to be allowable and the case in condition for allowance, which action is respectfully requested. Should the

Appl. No: 09/759,089
Amdt. Dated June 9, 2005
Reply to Office action mailed: April 12, 2005

Examiner be of the opinion that a telephone conference would expedite the prosecution of this case, the Examiner is requested to contact Applicants' attorney at the telephone number listed below. Any fee deficiency associated with this submittal may be charged to Deposit Account No. 50-1123.

Respectfully submitted,

June 9, 2005



Stuart T. Langley, No. 33,940
Hogan & Hartson LLP
One Tabor Center
1200 17th Street, Suite 1500
Denver, Colorado 80202
(720) 406-5335 Tel
(303) 899-7333 Fax